Usable Security and User Training

KAMI VANIEA
JANUARY 25
Think about it:
Is the Doodle link to the right secure?

Sign up for tutorial sessions

http://doodle.com/poll/t7ia4mbv9vk8ekec

Link is also available on the website, which is at:

http://www.inf.ed.ac.uk/teaching/courses/cs/
First, the news...

- And someone messes up SSL certs again...
  - http://www.theregister.co.uk/2011/08/29/fraudulent_google_ssl_certificate/
Quick explanation of SSL
We will cover this in more detail later
Slides with this background are from a talk given at the Royal Society Frontiers of Science event on why encryption is not adopted at scale
Encryption *(in transit)* properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
   - No one can read what you sent
   - No one can change what you sent

2. Knowing **who** you are communicating with
   - You are talking to who you think you are talking to and not someone else
Alice wants to talk securely with Bob
She can encrypt the connection (1)
But how can Alice know she is talking to Bob and not talking to Eve? (2)
Man in the middle attack
Alice goes to her favorite coffee shop and tries to visit BBC News
Osborne unveils sugar tax on soft drinks

George Osborne unveils a tax on the makers of soft drinks - and warns of the risks of leaving the EU in his eighth Budget.

© 20 minutes ago | UK Politics

Budget key points: At-a-glance

‘On course for a surplus’
Free Wi-Fi
From our friends at Google

I agree to the Terms of Service and have reviewed the Google Privacy Policy

Need help? 855-446-2374
Benign Main-in-the-Middle
https://ally.com

versus

http://ally.com
http versus https
Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
   - No one can read what you sent
   - No one can change what you sent

2. **Knowing who** you are communicating with
   - You are talking to who you think you are talking to and **not someone else**
Key management

Public/private key pairs

- Give public keys to other people
- Keep private keys private
- Verify other people's public keys

Keys are linked to identities

- A private key should NEVER be shared, so only one entity theoretically has access to it

Possession of a private can be cryptographically proven when starting a communication IF you have the public key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFHMqzgABCAC9NYUDD8KDLD3VHaIYw/4eRh6su4HLMp+J0+HULtEVLtUZj0XUWxH
KzoH8f7l9v/9Xoob8s93zzxsXKcg3MSEGE02b6f9lGofaVeSB4jwpoJ8HWNwslB
B79zmp6qg1Kch3QxvHLyr9T7709s5cPMeshU92zhek8g63mtnjB8Pw4t10
1ggkMDQbep2H2wv2RFRYy5zDouetekolFfLy0979kk1nE1e6894w9m1q0sZ
QYQExS+M5k+ckBc+4+R9H6d1m7EG9VHW0F4u50y20feoYjopfakkR7u3359vhN
8b/t7+mGMO2QUL2QBDss7w7Q7HqYylX3JdOABEB084G5r2w9gF5wXwH1nr
dmfuaWvHqQn54Z5C5Syh51a5bAT8EEw6EIAEFAKvNkYEvEccFMQj64vA5YH0iwki
BwMC4AQQV4UegFqIDQAeQaXkKACRCtRdssX/9HFICG/CAnwkuKay3e4qew
GWH56kCGy0HqOy3qWZ3hpy2mZjQkge1aX11sD0Bz+G75S+teZgK0nR0PF9G
F4Q2DEmadF18FPC3J5oZ6z6PD0B889qwhMy797678gY3E5Z0fu3ve0x23q0c5wT-
5svxVt+DKH9Qc257T5P2x9yq/XTLtsb4NhQPCoTDq8BhJ+VpsRX7yTaeaf
JaNhXo/1+L3HCQyf9zct4gb6wMMrFB/2ZC2D1oq4u266F4z2hsnM6Qnd4f
YQG5seWmflvEw2sob6z1aEav9F8Wjvbn8yH70s0E0cN0Yj2QeK2z20w4e26T
Ytrp0wCtE31LLlWfpfZmtnnYIYs0a2fUa8WZ2p2WY29p9okPokBTQGAJAla
BlwUICYWbYlgCQzAhWvBh1UAgk1Qg3wQB7d3g1hAXkBQwCNMc4nAbA02NEJ2
ZGx2s8j3hJAAWVnYyfr6slY69wB99f5GtuTD0X0a1L7F7QOWQmY2d5AFjY6Cm+
XBY1bA15uAaAhteFyaX3sM2n3qHz07y4EG0G8u00Wedhwp0qPRtLQJD1SL5M
Bilaww0K0vWbi9Be4ekMaIXCn5BFsBxe0Ah4RL2v1S5205dVn5IiC3KoxtubU7tL7m
ncL7wOrbrLdekuOhhWdn3s5yo/vpkHjDP0/ETYrEwED0yq32y/6wVQefb3keYy6zoN0
2wbdJusTo+p/PRx4jUjMDc0wYtF/srs/P39D0ZNB4c+h0vDPM7uOjxeu3zh
pzbv3e7Vhrh9nWizhBv/2tX134R7WMROMAwjHeEwECAAYAF1TpnSeAPcGqyVym
pp99LB2B/-z0psxsOqXb/Bhuy4777v1Dw3oFa31bVn7yXe/Yx3/gfjpf3t3w
XnnFLruuuy1vE3NWEtR0QmyQvR/5vJwblTQ7j0c5hjhhKhI7ECQ3DTRbOw
2un3iQGj23O3C2B3JucwEwsef1x79P1/9vP4+26bLkRD0pasb2bqtbpHmmVYkL
4QjBFH1YjUsjwo2Jh10hYp9Fzd2e1meoDeeEvkH6839NBN58WB6ekj2SKL
ZQcEPB8h4R9m88n6e6Wp6WpWyUwIVOnlMr8R09GBF4Bjw7w8WSL8BhG2EwKdO
Yq2yv9ZkArKX5w4+KUK1KD5fOC7CN7wq7Vlme68bcz3HR5PW217VMyrdRw8uUs0
INV1LUS3h+HzyyPz07Y6wGscb6T5K/IBy0bVYrBf7fwjy9f7weyfVId994
mzP700vori3G3s3s7gPB2B2JnWjMGy31Azx1zvRnuruqkYkvKFM2wEVjyuN
VN/c3WJh9FLwKDB0za0p2+z1mePGx0yVnem20z17Bspq2x0m02dMN2LwLc97
fHrBPsuUyGsYTA5S0I51dRk6Xog19e8hUv3vYqDqcO8kK4qy9gQmd8cta
P/FadyApQh8nW6qefgK+4QsRv5aue9B6h1eRpsDKM6kP3YMFmu58BOcAlOxycy
QZ6sYsz2c71D6pGhmp04U63pP7/SEwBhNKn0A4uV2jv2-8Dp/V07yQ2cy
42c7/vWvXeB1JTlarkG6esC16TQ1SsIUk4T3l05cB6t6vq6bQ8jsjG1uTWF
5yus0JyS26pFkN6P/2eH0NjxzJuLZud8tBhU9bMn/u0/pO DNAE0wvfnkVMAHma+R
Zq2e69uNjyR2v3szu3uWvUwFyJ3DE3A1F96Xh/S65Tulu3rHHNwpklMcjZhuHU
QDQDEAExk+X0PZz5wS2zaf1w20q69l1YfAf6L6tpxsSlk4zS7pNq3pFjD3OC7T
2J7Oh9N9XGUKorPSKj8R6Qog5MEAEe4YbBQQYQJyowDUCU0cycUy
sGACLKVRdssX/9HZS+HB/9BzDsSmigLcHfH7p1JwKkzL558wMVjEgLMjQLZ
Hw2y/m3sApeGy17Fnu916400jwZqU5/djW9iluuK170ypP+DUU995GOSu3m
mC8EnGWYb0xftVmGv00oOeO272TUsFvsApxvBDYkR8BO7THKwF0z03Hk0wD
TgAFJQD23e6cb0fK2by7feV5AQpR0oczvBn0s3J9W0B385yvd
R0Bx8s/3Q0g7HukJ6f2v3XoWunI6wF5kRg3BluwHfPlHHwWfemmSs/aQb
YK93g9vHyacaS3jbg0qVLazWSWwh6vVfIE2BFy/Ed
-----END PGP PUBLIC KEY BLOCK-----
```
Idea: Certificate Authorities can do the verification instead of users
Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Suporfish may make it trivial for attackers to spoof any HTTPS website.

victim

web server

attacker

This certificate is intended for the following purpose(s):
• All application policies

Issued to: internetbanken.privat.nordea.se

Issued by: Superfish, Inc.

Valid from 09/01/2014 to 16/03/2015
hey @Gogo, why are you issuing *.google.com certificates on your planes?
Real world click-through rates

- Studied the click-through rate for malware and HTTPS warnings
  - **Malware**
    - Firefox 7.2%
    - Chrome 23.2%
  - **Phishing**
    - Firefox 9.1%
    - Chrome 18.0%
  - **HTTPS**
    - Firefox 33.0%
    - Chrome 70.2%

Click through rates based on if the user had visited the site in the past

Users are ignoring warnings for sites they have visited in the past.

Why do people click through the warnings?

- The site is used often and trusted
  - “YouTube is a well known site. I’d assume that the malware block is in error.”
- The person who posted the link is trusted
  - “I find it harder to believe [the warning] when my facebook friend just posted it and had no problems.”
- The site where the link is assumed to have good security
  - “I presume that visiting youtube from a facebook link would be safe.”
- They think they are safe
  - “I use Linux I’m not afraid of anything.”
  - “I have an anti virus”
Why people don’t use privacy protections

1. People don’t really care about privacy
2. People are not aware of the privacy issues
3. People are not aware of how to protect themselves
4. People are aware, but are unable to use the privacy protections
Communication-Human Information Processing Model (C-HIP)

- Developed to model why people do or don’t understand road signs
- We adapted it to computer security
Human In the Loop Framework

Communication

Communication Impediments
- Environmental Stimuli
- Interference

Human Receiver

Personal Variables
- Demographics and Personal Characteristics
- Knowledge and Experience

Communication Delivery
- Attention Switch
- Attention Maintenance

Communication Processing
- Comprehension
- Knowledge Acquisition
- Knowledge Retention
- Knowledge Transfer

Intentions
- Attitudes and Beliefs
- Motivation

Capabilities

Behavior
We are now going to use the framework to figure out why people are ignoring SSL warnings...
What level of the framework does this fail at?
And this one?
And this one?
Any better?

The Website Ahead Contains Malware!

Google Chrome has blocked access to youtube.com for now.

Even if you have visited this website safely in the past, visiting it now is very likely to infect your computer with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

Go back Details about problems on this website Proceed at your own risk

- Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy

[Diagram showing human receiver pathways and variables: Personal Variables, Communication Delivery, Communication Processing, Application, Capabilities, Demographics and Personal Characteristics, Attention Switch, Attention Maintenance, Comprehension, Knowledge Acquisition, Knowledge Retention, Knowledge Transfer, Intentions, Attitudes and Beliefs, Motivation]
And this one?

- The site is used often and trusted
  - “YouTube is a well known website. I’d assume that the malware block is in error.”

- The person who posted the link is trusted
  - “I find it harder to believe [the warning] when my Facebook friend just posted it and had no problems.”

- The site where the link is assumed to have good security
  - “I presume that visiting youtube from a Facebook link would be safe.”

- They think they are safe
  - “I use Linux I’m not afraid of anything.”
  - “I have an anti virus”
Users
Users are not the enemy

- Malicious actors are the enemy
- Users are a partner in keeping the system secure
- Like any partner:
  - They have skills you don’t have
  - They are missing skills you do have
- Think about what skills they have that you need
- Use the skills you have to make good decisions on users’ behalf
Phishing attacks and training
Phishing

- Phishing – Attempting to trick someone into taking the “bait” and interacting in a way they should not.
  - Typically involves the impersonator pretending to be someone else that the person trusts
  - Interactions: Clicking a link, opening a file, replying with information, transferring money, etc.
- Spear phishing – Phishing, but with a small number of targets and each email is crafted for that individual
- Whaling – Phishing for people with a lot of money, i.e. CEO
- QRishing – Phishing attacks through QR codes
What on this email can be trusted?

From: "Fletcher, Freya" <ffletcher@conejousd.org>

Subject: FW: ITS Administrative Support

To: undisclosed-recipients;

From: Fletcher, Freya
Sent: Thursday, March 05, 2015 4:47 AM
Subject: ITS Administrative Support

Dear User,

Your password will expire within 24hrs Click on: Staff & faculty update to validate your e-mail.

This email has been scanned by the Symantec Email Security.cloud service. For more information please visit http://www.symanteccloud.com

http://staffupgrade.moonfruit.com/
(Wrong) Trust indicators

Authority figure that often sends emails to do things

Clear threat to recipient’s ability to log in

(False) statement saying the email has been scanned and is safe
Sneaky email to get the recipient to open the attachment, which is an html document.
Problem: Users click on links and attachments

- Scan all incoming attachments and links for blacklisted content
- Teach users
  - Only click if you are expecting the email
  - Do not open attachments unless you are expecting them
  - If you are not sure, contact the person or company separately and ask if they sent the email
  - If you are not sure, contact the IT department
  - Banks and credit card companies will never contact you this way
Anti-Phishing Phill

- Serious game to help people learn to spot dangerous URLs
- Training sometimes works
- But it takes time
- And people forget
PhishGuru

- Comic to train people to spot phishing attacks
- Best time to train is after a user has already fallen for an attack
- Send out fake attacks and train those who click on them
Give users options that make sense and work for them
PhishGuru

- Users know what they are expecting
- Users know who the email looks like it is from
- Users can do an out-of-band contact (phone call)
- Users do not want to ignore a serious issue
In Summary...

• Academics say in-the-moment training works

• Chief Security Officers (CSOs) have mixed opinions

• Everybody thinks that users clicking on links and attachments is a big problem
Why show warnings at all?

• Determined users might disable Safe Browsing. Which would prevent future warnings.

• User could also open the website in another browser that is less safe and does not block the website.
  ◦ America Online users used to go to a friend’s house to open malicious sites because the ISP blocked malicious sites.
  ◦ Different browsers block different sets of sites, we don’t want to teach users to use less safe browsers.
Questions